ICO consultation on the draft right of access guidance

The right of access (known as subject access) is a fundamental right of the General Data Protection Regulation (GDPR). It allows individuals to find out what personal data is held about them and to obtain a copy of that data. Following on from our initial GDPR guidance on this right (published in April 2018), the ICO has now drafted more detailed guidance which explains in greater detail the rights that individuals have to access their personal data and the obligations on controllers. The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the exemptions that are most likely to apply in practice when handling a request.

We are running a consultation on the draft guidance to gather the views of stakeholders and the public. These views will inform the published version of the guidance by helping us to understand the areas where organisations are seeking further clarity, in particular taking into account their experiences in dealing with subject access requests since May 2018.

If you would like further information about the consultation, please email SARguidance@ico.org.uk.

Please send us your response by 17:00 on **Wednesday 12 February 2020**.

Privacy statement

For this consultation, we will publish all responses received from organisations but we will remove any personal data before publication. We will not publish responses received from respondents who have indicated that they are an individual acting in a private capacity (e.g. a member of the public). For more information about what we do with personal data see our privacy notice.

Please note, your responses to this survey will be used to help us with our work on the right of access only. The information will not be used to consider any regulatory action, and you may respond anonymously should you wish.

Please note that we are using the platform Snap Surveys to gather this information. Any data collected by Snap Surveys for ICO is stored on UK servers. You can read their Privacy Policy

Q1 Does the draft guidance cover the relevant issues about the right of access?

- ☒ Yes
- ☐ No
- ☐ Unsure/don't know

If no or unsure/don't know, what other issues would you like to be covered in it?

Q2 Does the draft guidance contain the right level of detail?

- ☒ Yes
- ☐ No
- ☐ Unsure/don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Q3 Does the draft guidance contain enough examples?

- ☐ Yes
- ☒ No
- ☐ Unsure/don't know

If no or unsure/don't know, please provide any examples that you think should be included in the draft guidance.

It would be good to see 3rd party Claims Management Company (CMCs) examples in a couple of the sections of the guidance.

For example, within pages 21/22, which deals with how firms should deal with bulk requests. In this section, it would also be helpful for the ICO to clarify the authorisation process i.e. Letters of Authority (LOA) are needed and how long they last before it's reasonable to go back and ask the CMC or other third party representative to get an up to date LOA (e.g. six months or a year etc.) In this section, we are also concerned that the guidance states that the behaviour of third parties shouldn't be taken into account in determining whether a request is 'manifestly unfounded' or 'excessive'. We think firms should be able to consider the conduct of the CMC when judging whether a DSAR request is 'manifestly unfounded'. Given the poor practice of some CMCs, and the resulting risks to customers (not least the risk that their personal data is being misused) we think that firms ought to be able to consider the CMCs conduct too.

We agree with the ICO that it would also be helpful to have a range of examples between pages 35-38 which look at 'manifestly unfounded' and 'excessive requests'. For example, where a CMC only wants to know if their client/s have PPI then a full DSAR request is likely to be 'excessive'. The onus in such cases should be on the CMC to make targeted requests and this should be made clear in this guidance. A failure to do so would give CMCs excessive amounts of data which could be vulnerable to an unnecessary data breach.

Q4: We have found that data protection professionals often struggle with applying and defining 'manifestly unfounded or excessive' subject access requests. We would like to include a wide range of examples from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive requests below (if applicable).

See response to Q3 above.

The consumer-facing financial services sector has seen a significant increase in volume of data subject access requests. Whilst the intention of the data protection regime (whether in the form of the GDPR or Data Protection Act 2018) is intended to allow a data subject a right of access to his personal data in order to consider the lawfulness of the processing, the reality is that individuals (or representatives of individuals) are using/ exploiting this right for other purposes, and often with litigation in mind. For example: individuals generally use this right to obtain information and material from financial services institutions in order to trigger a claim against the institution or to bolster a claim that is already underway.

UK national case-law generally allows for this and suggests that data controllers should deal with DSARs in a "motive blind" manner. However, this position and case-law was decided before the volume increase that has been seen under the GDPR. The volume is excessive, and often financial services providers can receive hundreds of DSAR requests on a given day. This volume actually acts against the stated aim of the DSAR regime, of allowing data subjects to consider the lawfulness of the processing, as it cannot be expected that data controllers aptly manage such a large volume of requests.

It must also be borne in mind that often only a small percentage of DSAR requests are true requests for data protection purposes, and will regularly be more akin to a request for information or documentation. Large volumes of DSAR requests lead to delays and incomplete responses as a result. It is telling that often incomplete responses (e.g. those that provide key information or documentation most pertinent to the circumstances giving rise to the DSAR) are often accepted or go unchallenged.

In addition, we have heard of numerous occasions where the data subject's representative has demanded money in settlement of a complaint or claim, and suggested that a failure to make the payment would lead to the issuing of a DSAR. This is likely because it is known and understood that the administrative burden of fully complying with a DSAR request can exceed the value of the payment demand.

Therefore, as suggested in response to Q3 above, the importance of more targeted SARs/information requests would be a good example. For example, if a CMC/3rd party is only interested in whether their customer/client has PPI or not then it would be helpful for this guidance to guide CMCs, through examples, towards more targeted SARs. It may also be helpful for this guidance to highlight the dangers of requesting and holding excessive amounts of data on their clients.

In addition, the case law set out in Ittahadieh and Dawson Damer judgments, considered the DSAR regime (albeit under the DPA but with the relevant provision unchanged under the GDPR) and established that the obligation was to undertake "*a reasonable and proportionate*" search for personal data. These judgments recognise limits to what controllers can realistically do with respect to the searching of volumes of personal data held. This should be recognised by the ICO in its guidance, which generally currently states that "all" personal data must be provided.

The current guidance states that "*you must consider each SAR within a bulk request individually and respond appropriately*". This is problematic given the volume of requests currently being received. Controllers are unable to comply with the subject access elements of the data protection regime with the wording in this current form. Amending the wording as follows would allow for controllers to properly consider and comply with DSARs, whilst remaining wholly consistent with the GDPR and Data Protection Act 2018:

"*You should consider each SAR within a bulk request individually and respond appropriately. You may consider the volume of SARs made as part of a bulk request as potentially providing a reason for extending the time-limits for response to up to 3 months, under Article 12(3) of the GPDR".*

Q5 On a scale of 1-5 how useful is the draft guidance?

1 – Not at all useful	2 – Slightly useful	3 – Moderately useful	4 – Very useful	5 – Extremely useful
☐	☐	☒	☐	☐

Q6 Why have you given this score?

We think that if some of the suggestions in our response were added the guidance would become 'very useful'. As currently written, it doesn't stop less scrupulous CMCs/3rd party representatives from exploiting the legitimate use of the SARs process and 'weaponising it' for litigation purposes.

It is important consumers can check what information and data firms have on them. But if the only aim is to check whether or not they have a certain product e.g. PPI, then this is all that should be requested and indeed provided.

Further, it is often demonstrated that CMCs or other claimant litigation firms, far too readily rely upon DSARs as a means of information and data gathering to advance a claim. The ICO Guidance must bear in mind the regulatory standing of the requester. According to the FCA Guidance for Claims Management Companies they are under a regulatory requirement to have appropriate levels of engagement with their client, and to exercise due diligence before advancing a claim. The over-reliance upon DSARs is a dereliction of this duty, encouraging CMCs to avoid simple interaction and data gathering from its clients. In addition, solicitors who are seeking to pursue litigation must comply with the Civil Procedure Rules (CPR), and ought to be providing a defendant with sufficient information, detail and supporting document in its letter of claim. The ICO Guidance in its current form does not refer or mention these other regulatory duties, and the over-reliance and use of DSARs amongst data subject's representatives has effectively switched the burden of information gathering and preparing a claim.

Accordingly, we consider that guidance and/or clarification by the ICO relating to the interaction between civil litigation rules, CMC regulation, and the DSAR regime would be highly instructive. In particular, we consider that understanding the ICO's position with respect to unfounded or 'weaponised' DSAR requests (which have clear motives which are not merely related to the protection of subject rights) would assist controllers in these circumstances.

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
☐	☐	☐	☒	☐

The guidance is clear and easy to understand/navigate and will be particularly useful for those who do not deal with SARs on a daily basis. However, as alluded to above, in order to make it more useful all CMC abuses need to be addressed. We believe this could be achieved by addressing some of the issues raised above e.g. more guidance around LOA's, the ability to challenge detrimental behaviours by some CMCs and promoting more targeted SARs/DSARs, where appropriate. For example: as DSARs are submitted in bulk, and often as a means of finding out if a data subject is a customer of the respondent, many DSARs are submitted in which the respondent holds no data about the individual. The current ICO Guidance expects the respondent to still respond to such a DSAR, albeit on brief terms. However, there is no consequence or punishment for the mass submission of DSARs when there is no justification or cause. The guidance lacks any deterrent for such behaviour, which ought to be considered as 'manifestly unfounded and excessive'.

On the point of more targeted SARs/DSARs, we have concerns about the current limitations placed on firms when it comes to dealing with broad untargeted requests from data subjects, which are often made when the real intention is to merely obtain information regarding a limited set of data (e.g. does the data subject have PPI). Clearly, if the data subject wants 'all data', they should receive exactly that, regardless of the cost implications for firms. However, in our members' experience, in many such cases it is to the benefit of the data subject for she/he to receive targeted information, rather than have to look for the 'needle in a haystack' of data. The current guidance, in particular the fixed time limit for responses, restricts the ability of firms to engage with the data subject with a view to focusing the scope of a request. In our view, it would be helpful if the guidance reverted to the previous format, which permitted time for responding to the SAR to be extended to allow the firm to attempt to engage the data subject, but with the addition of a proviso that full disclosure would be required if the data subject failed to agree a limited scope within an extended period (which would include cases in which the data subject simply failed to engage with the firm on this point). We feel this would amount to a balanced approach, working to the benefit of both firms and data subjects.

We believe that more targeted SARs could also be achieved by this ICO guidance if the ICO suggested the basis for a data subject making a DSAR with reasons/examples such as:

- The data subject believing the data to be misused or mis-represented and explaining the reason for that belief;
- Requiring data for a specific purpose, such as checking the validity of a credit agreement, or information from the point of sale to assess an affordability complaint or a product query (e.g. whether they have PPI);
- Believing the personal data is being processed without consent and explaining the reason for that consent;
- Or if all information is required, give a reason for needing all the information requested.

Alternatively, the ICO has previously suggested that some industry sectors could service large volumes of DSARs by taking steps such as creating online portals for access to data. Perhaps guidance from ICO on the availability for use of such portals would be valuable.

There may also be other reasons/examples, but the point is that the above would allow firms, in the first instance, to provide specific relevant information in response to the need for personal data being requested. If having been provided the information does not meet with the data subjects need for it, of course further information could still be provided.

Finally, some member firms are receiving standard template letters by CMCs that make a s77 request (this is an entitlement to receive a statement of account and copy of the credit agreement (for example, for a personal loan), a DSAR request and complaint all within the same letter. This is clearly not the objective of a DSAR/SARs request, not least because a complaint is a separate issue governed by the FCA's DISP rules (which govern how firms deal with complaints). But again, this goes back to some CMC behaviours and is addressed in our response to Q3 above.

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

Q9 Are you answering as:

- ☐ An individual acting in a private capacity (e.g. someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

Finance & Leasing Association (FLA)

What sector are you from:

Financial Services (consumer credit, motor and asset finance)

Q10 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☐ ICO website
- ☒ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other

Thank you for taking the time to complete the survey.